

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-176637
 (43)Date of publication of application : 21.06.2002



(51)Int.Cl. H04N 7/173
 G06F 15/00
 G06F 17/30
 G06F 17/60

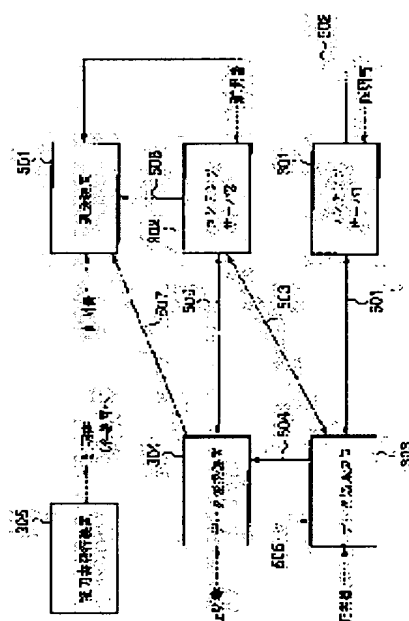
(21)Application number : 2000-370345 (71)Applicant : CANON INC
 (22)Date of filing : 05.12.2000 (72)Inventor : WAKAO SATOSHI

(54) DATA DISTRIBUTION METHOD AND ITS SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data distribution method and a data distribution system that can automatically impose charging on a user accompanying acquisition and conversion of contents data by the user, in addition to the authentication of the user.

SOLUTION: The data distribution system is configured, with at least a user terminal 303 and contents servers 301, 302 being interconnected via a network and the contents servers distributes contents data to the user terminal upon the request of the user terminal 303. The data distribution server is provided with a certificate issue device 305, that is connected to the user terminal and the contents servers via the network and issues digital identification information to the user terminal and the contents servers, with a data converter 304 that converts the content data into data, in a form that can be processed by the user terminal, and a charging device 501 that conducts charging corresponding to the distribution of the contents data and the conversion of the contents data upon the request from the contents servers and the data converter. The user terminal 303, the data converter 304 and the charging device 501 carry out transmission reception, only when mutual authentication on the basis of the digital identification information from the certificate issue device 305 is successful.



LEGAL STATUS

[Date of request for examination]
 [Date of sending the examiner's decision of rejection]
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]
 [Patent number]
 [Date of registration]
 [Number of appeal against examiner's decision of rejection]
 [Date of requesting appeal against examiner's decision of rejection]
 [Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-176637

(P2002-176637A)

(43)公開日 平成14年6月21日(2002.6.21)

(51)Int.Cl. ⁷	識別記号	F I	ターマコード*(参考)
H 0 4 N 7/173	6 4 0	H 0 4 N 7/173	6 4 0 A 5 B 0 7 5
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 Z 5 B 0 8 5
17/30	1 1 0	17/30	1 1 0 F 5 C 0 6 4
	2 4 0		2 4 0 C
17/60	Z E C	17/60	Z E C

審査請求 未請求 請求項の数17 O L (全 22 頁) 最終頁に続く

(21)出願番号 特願2000-370345(P2000-370345)

(22)出願日 平成12年12月5日(2000.12.5)

(71)出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72)発明者 若尾 聡

東京都大田区下丸子3丁目30番2号 キヤノン株式会社内

(74)代理人 100076428

弁理士 大塚 康德 (外2名)

Fターム(参考) 5B075 PQ02 PQ04 PQ05

5B085 AC04 AE23 BC07

5C064 BA01 BA07 BB01 BB07 BC01

BC07 BC16 BC18 BC20 BC23

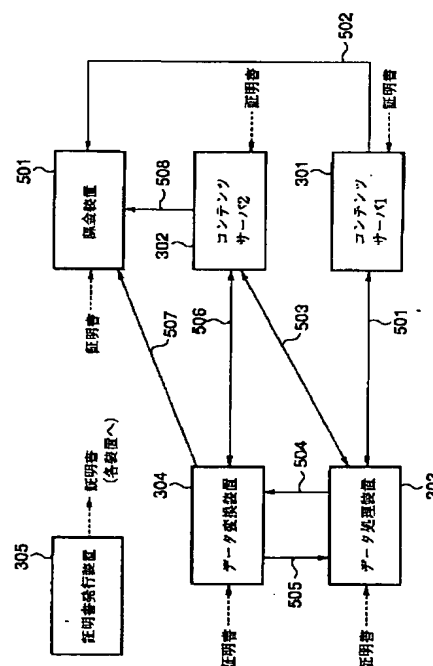
BD02 BD08

(54)【発明の名称】 データ配信方法及びそのシステム

(57)【要約】

【課題】 ユーザの認証に加えて、そのユーザによるコンテンツデータの取得及びデータ変換に伴う課金を自動的に行う。

【解決手段】 少なくともユーザ端末303とコンテンツサーバ301、302とがネットワークを介して接続され、ユーザ端末303からの要求によりコンテンツサーバからユーザ端末にコンテンツデータを配信するデータ配信システムであって、ネットワーク介して接続され、ユーザ端末及びコンテンツサーバに対してデジタル識別情報を発行する証明書発行装置305と、ユーザ端末303からの要求に応じて、コンテンツデータを当該ユーザ端末が処理可能な形式のデータに変換するデータ変換装置304と、コンテンツサーバ及びデータ変換装置からの要求に応じて、コンテンツデータの配信及びコンテンツデータの変換に対応する課金を行う課金装置501とを有し、ユーザ端末303、データ変換装置304及び課金装置501は、認証装置305からのデジタル識別情報に基づく相互認証に成功した場合にのみ送受信する。



1

【特許請求の範囲】

【請求項 1】 少なくともユーザ端末とコンテンツサーバとがネットワークを介して接続され、前記ユーザ端末からの要求により前記コンテンツサーバから前記ユーザ端末にコンテンツデータを配信するデータ配信システムであって、

前記ネットワークを介して接続され、前記ユーザ端末及びコンテンツサーバに対してデジタル識別情報を発行する認証装置と、

前記ユーザ端末からの要求に応じて、コンテンツデータを当該ユーザ端末が処理可能な形式のデータに変換するデータ変換装置と、

前記コンテンツサーバ及び前記データ変換装置からの要求に応じて、前記コンテンツデータの配信及び前記コンテンツデータの変換に対応する課金を行う課金装置とを有し、

前記ユーザ端末、前記データ変換装置及び前記課金装置は、前記認証装置からの前記デジタル識別情報に基づく相互認証に成功した場合に送受信することを特徴とするデータ配信システム。

【請求項 2】 前記ユーザ端末は、前記コンテンツサーバに要求した前記コンテンツデータが当該ユーザ端末で処理不可能な場合、前記データ変換装置に対して当該コンテンツデータを、当該ユーザ端末が処理可能な形式のデータに変換するように要求することを特徴とする請求項 1 に記載のデータ配信システム。

【請求項 3】 前記課金装置は、課金を行うため必要となるデータを前記コンテンツサーバ及び前記データ変換装置から受信する受信手段と、前記受信手段により受信された前記データに基づいて課金データを生成する課金データ生成手段と、前記課金データを登録する課金データベースと、を有することを特徴とする請求項 1 又は 2 に記載のデータ配信システム。

【請求項 4】 前記認証装置は更に、前記ユーザ端末、前記コンテンツサーバ及び前記データ変換装置からのデジタル識別データ発行要求を受信する受信手段と、

前記受信手段により受信された発行要求を送信した前記ユーザ端末、前記コンテンツサーバ又は前記データ変換装置に対してデジタル識別データを発行するかどうかを判断する判断手段と、

前記判断手段により発行すると判断された前記ユーザ端末、前記コンテンツサーバ又は前記データ変換装置に対する前記デジタル識別データを発行する発行手段と、前記デジタル識別データを登録する登録手段と、

前記発行手段により発行されたデジタル識別データを当該前記ユーザ端末、前記コンテンツサーバ又は前記データ変換装置に送信する手段と、を有することを特徴とする請求項 1 に記載のデータ配信システム。

2

【請求項 5】 前記コンテンツデータは、MPEGデータであることを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載のデータ配信システム。

【請求項 6】 前記認証装置は、更に、前記登録手段に登録された前記デジタル識別データを無効化する指示を受信すると、前記登録手段に登録された、対応するデジタル識別データを削除することを特徴とする請求項 4 に記載のデータ配信システム。

【請求項 7】 少なくともユーザ端末とコンテンツサーバとがネットワークを介して接続され、前記ユーザ端末からの要求により前記コンテンツサーバから前記ユーザ端末にコンテンツデータを配信するデータ配信システムにおけるデータ配信方法であって、

前記ネットワークを介して接続され、前記ユーザ端末及びコンテンツサーバに対してデジタル識別情報を発行する工程と、

前記ユーザ端末からの要求に応じて、コンテンツデータを当該ユーザ端末が処理可能な形式のデータに変換するデータ変換装置によりデータを変換する工程と、

前記コンテンツサーバ及び前記データ変換装置からの要求に応じて、前記コンテンツデータの配信及び前記コンテンツデータの変換に対応する課金を課金装置により行わせる課金工程とを有し、

前記ユーザ端末、前記データ変換装置及び前記課金装置は、前記デジタル識別情報に基づく認証に成功した場合に送受信することを特徴とするデータ配信方法。

【請求項 8】 前記ユーザ端末は、前記コンテンツサーバに要求した前記コンテンツデータが当該ユーザ端末で処理不可能な場合、前記データ変換装置に対して当該コンテンツデータを、当該ユーザ端末が処理可能な形式のデータに変換するように要求することを特徴とする請求項 7 に記載のデータ配信方法。

【請求項 9】 前記課金工程で、課金を行うため必要となるデータを前記コンテンツサーバ及び前記データ変換装置から受信する受信工程と、前記受信工程で受信された前記データに基づいて課金データを生成する課金データ生成工程と、を有することを特徴とする請求項 7 又は 8 に記載のデータ配信方法。

【請求項 10】 前記デジタル識別情報は、前記ユーザ端末、前記コンテンツサーバ及び前記データ変換装置からのデジタル識別データ発行要求に基づいて発行されることを特徴とする請求項 7 に記載のデータ配信方法。

【請求項 11】 前記コンテンツデータは、MPEGデータであることを特徴とする請求項 7 乃至 10 のいずれか 1 項に記載のデータ配信方法。

【請求項 12】 前記デジタル識別データを無効化する指示を受信すると対応するデジタル識別データを削除する工程を更に有することを特徴とする請求項 7 に記載のデータ配信方法。

3

【請求項 13】 少なくともユーザ端末とコンテンツサーバとがネットワークを介して接続され、前記ユーザ端末からの要求により前記コンテンツサーバから前記ユーザ端末にコンテンツデータを配信するデータ配信システムにおけるデータ配信方法であって、

前記ユーザ端末及びコンテンツサーバからの要求に応じて、各対応するデジタル識別情報を発行する工程と、前記ユーザ端末から前記コンテンツサーバに対してコンテンツデータを要求する工程と、

前記要求に応じて前記コンテンツサーバから、要求したユーザ端末に前記コンテンツデータを送信する送信工程と、

前記コンテンツデータが前記ユーザ端末が処理可能な形式のデータでない場合に、当該ユーザ端末が処理可能なデータ形式のデータに変換するデータ変換工程と、前記コンテンツデータの配信及び前記コンテンツデータのデータ変換に対応する課金を行う課金工程とを有し、前記送信工程、前記データ変換工程及び前記課金工程は、前記デジタル識別情報に基づく認証に成功した場合に実施されることを特徴とするデータ配信方法。

【請求項 14】 前記課金工程では、課金を行うため必要となるデータを前記コンテンツサーバ及び前記データ変換工程から取得する取得工程と、前記取得工程で取得された前記データに基づいて課金データを生成する課金データ生成工程と、前記課金データを課金データベースに登録する工程と、を有することを特徴とする請求項 13 に記載のデータ配信方法。

【請求項 15】 前記ネットワークに接続された各端末、サーバ及び装置に対応する前記デジタル識別データは、それぞれ対応する各端末、サーバ及び装置からの発行要求に基づいて発行されることを特徴とする請求項 13 に記載のデータ配信方法。

【請求項 16】 前記コンテンツデータは、MPEG データであることを特徴とする請求項 13 乃至 15 のいずれか 1 項に記載のデータ配信方法。

【請求項 17】 各端末、サーバ及び装置に対応する前記デジタル識別データを無効化する工程を更に有することを特徴とする請求項 13 に記載のデータ配信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークを介して接続されたユーザ端末からのコンテンツデータの要求に基づいて、コンテンツデータを各ユーザ端末に配信するデータ配信方法及びそのシステムに関するものである。

【0002】

【従来の技術】近年、動画像や音声などのデータを符号化し、それぞれの符号化データをオブジェクトとして扱い、これら所謂マルチメディアデータを組み合わせて単

4

一のビットストリームとして伝送する手法として、ISO にて MPEG-4 (Moving Picture Experts Group part 4) が標準化されつつある。この MPEG-4 により符号化されたコードを受信して復号する受信側（再生側）では、例えば、音声と動画シーンを関連付けて再生する。このような MPEG-4 コードを処理するシステムにおいては、データがオブジェクトとして扱われるという特性のために、受信したビットストリームを、オブジェクト毎に 1 つ 1 つバラバラにして容易に再編成できる。上述したような MPEG-4 のデータストリームでは、これまでの一般的なマルチメディアストリームとは異なり、いくつもの動画シーンや動画オブジェクトを、単一のストリーム上でそれぞれ独立して送受信することができる。また音声についても同様に、いくつものオブジェクトを単一のストリーム上で独立して送受信する機能を有する。

【0003】これらのオブジェクトを合成して、あるシーンを合成するための情報として VRML (Virtual Reality Modeling Language) を修正したシーン記述情報

(BIFS: Binary Format For Scenes) が存在する。この BIFS は、シーン記述情報が 2 値で記述されているもので、この BIFS に従って各シーンが合成される。このような、シーンの合成に必要な個々のオブジェクトは夫々、個別に最適な符号化が行われて送信されることになるので、復号側でも個別に復号され、BIFS の記述に従い、個々のデータの持つ時間軸を再生装置内部の時間軸に同期させてシーンを合成、出力することになる。

【0004】又、供給されるオブジェクトを復号装置が、そのオブジェクトを復号して再生される音声や映像を視聴する権利を有しているか否かが、伝送される IPMP (Intellectual Property Management and Protection) 情報に基づいて判断される。

【0005】

【発明が解決しようとする課題】このように、一般の著作権管理システムでは、IPMP データを用いることにより、コンテンツの不正な使用を防止することを可能にしている。しかし、コンテンツ使用に対する正当な対価を著作権者に支払う仕組みではない。この支払い（課金管理）を実現させるためには、誰がいつどんなコンテンツをどれだけ入手したかを把握するとともに、本当にその本人が入手を行ったのかを確認する（ユーザ認証）必要がある。

【0006】コンテンツの著作権者としては、上記のような不正防止及び課金管理等を含むシステムがあれば安心してコンテンツを提供することができるが、このようなシステムが無い場合には、コンテンツを提供することを躊躇することになる。即ち、ユーザ認証や課金システムを実現することは、ネットワークを使用したコンテンツ配信サービスのビジネスを立ち上げるため必要なもの

である。しかしながら上記のデータ変換システム及びIPMPシステムと連携したユーザ認証、課金システムは考えられていなかった。

【0007】本発明は上記従来例に鑑みてなされたもので、ユーザの認証に加えて、そのユーザによるコンテンツデータの取得及びデータ変換に伴う課金を自動的に行うことができるデータ配信方法及びシステムを提供することを目的とする。

【0008】又本発明の目的は、視聴を許可されたユーザだけがそのコンテンツデータを使用でき、かつ自動的に、そのユーザによるコンテンツデータの使用料を課金できるデータ配信方法及びシステムを提供することにある。

【0009】

【課題を解決するための手段】上記目的を達成するために本発明のデータ配信システムは以下のような構成を備える。即ち、少なくともユーザ端末とコンテンツサーバとがネットワークを介して接続され、前記ユーザ端末からの要求により前記コンテンツサーバから前記ユーザ端末にコンテンツデータを配信するデータ配信システムであって、前記ネットワーク介して接続され、前記ユーザ端末及びコンテンツサーバに対してデジタル識別情報を発行する認証装置と、前記ユーザ端末からの要求に応じて、コンテンツデータを当該ユーザ端末が処理可能な形式のデータに変換するデータ変換装置と、前記コンテンツサーバ及び前記データ変換装置からの要求に応じて、前記コンテンツデータの配信及び前記コンテンツデータの変換に対応する課金を行う課金装置とを有し、前記ユーザ端末、前記データ変換装置及び前記課金装置は、前記認証装置からの前記デジタル識別情報に基づく相互認証に成功した場合に送受信することを特徴とする。

【0010】上記目的を達成するために本発明のデータ配信方法は以下のような工程を備える。即ち、少なくともユーザ端末とコンテンツサーバとがネットワークを介して接続され、前記ユーザ端末からの要求により前記コンテンツサーバから前記ユーザ端末にコンテンツデータを配信するデータ配信システムにおけるデータ配信方法であって、前記ネットワーク介して接続され、前記ユーザ端末及びコンテンツサーバに対してデジタル識別情報を発行する工程と、前記ユーザ端末からの要求に応じて、コンテンツデータを当該ユーザ端末が処理可能な形式のデータに変換するデータ変換装置によりデータを変換する工程と、前記コンテンツサーバ及び前記データ変換装置からの要求に応じて、前記コンテンツデータの配信及び前記コンテンツデータの変換に対応する課金を課金装置により行わせる課金工程とを有し、前記ユーザ端末、前記データ変換装置及び前記課金装置は、前記デジタル識別情報に基づく認証に成功した場合に送受信することを特徴とする。

【0011】上記目的を達成するために本発明のデータ配信方法は以下のような工程を備える。即ち、少なくともユーザ端末とコンテンツサーバとがネットワークを介して接続され、前記ユーザ端末からの要求により前記コンテンツサーバから前記ユーザ端末にコンテンツデータを配信するデータ配信システムにおけるデータ配信方法であって、前記ユーザ端末及びコンテンツサーバからの要求に応じて、各対応するデジタル識別情報を発行する工程と、前記ユーザ端末から前記コンテンツサーバに対してコンテンツデータを要求する工程と、前記要求に応じて前記コンテンツサーバから、要求したユーザ端末に前記コンテンツデータを送信する送信工程と、前記コンテンツデータが前記ユーザ端末が処理可能な形式のデータでない場合に、当該ユーザ端末が処理可能なデータ形式のデータに変換するデータ変換工程と、前記コンテンツデータの配信及び前記コンテンツデータのデータ変換に対応する課金を行う課金工程とを有し、前記送信工程、前記データ変換工程及び前記課金工程は、前記デジタル識別情報に基づく認証に成功した場合に実施されることを特徴とする。

【0012】

【発明の実施の形態】以下、添付図面を参照して本発明の好適な実施の形態を詳細に説明する。

【0013】まず最初に、一般的なMPEG-4再生装置の構成と動作を説明する。

【0014】図1は一般的なMPEG-4再生装置（データ処理装置：ユーザ端末）の概略構成を示すブロック図である。

【0015】図1において、伝送路101は各種ネットワーク、コンピュータバス等のデータの路であり、MPEG-4ストリームが入力されるネットワークである。ここで、伝送路101は通信路の意味の他にCD-ROM、DVD-ROM、DVD-RAMといった記録媒体装置と再生装置とのインターフェースも意味する。

【0016】この再生装置では、ネットワークから配信されたMPEG-4データや、記録媒体装置から再生されたMPEG-4データは分離部102に入力される。ここでMPEG-4データは、シーン記述情報データ、動画像オブジェクトデータ、音声オブジェクトデータ、オブジェクト記述データ等に分離された後、それぞれのメモリ部103～106に入力される。

【0017】ここで、音声オブジェクトデータは例えば、周知のCELP (Code Excited Linear Prediction) 符号化や、変換領域重み付けインターリーブベクトル量子化 (TWINVQ) 符号化等の高効率符号化が施されたデータであり、動画像オブジェクトデータは、例えば、MPEG-4やH-263方式にて高効率符号化が施されたデータである。またオブジェクト記述データは、各オブジェクトに関する属性情報等を示すデータである。メモリ部104～106の各オブジェクトデータ

はそれぞれの復号部 108~110へ入力され、復号部 108~110において、上述のような高効率符号化された、動画像オブジェクトデータ、音声オブジェクトデータ、及びオブジェクト記述データ等が復号される。但し、メモリ部 103に入力されたシーン記述情報データのみは、シーン記述復号部 107へ直接入力されて復号される。

【0018】尚、図 1 においては音声オブジェクト、動画像オブジェクト、オブジェクト記述データについて、それぞれ複数の互いに異なる種類のオブジェクトが MP EG-4 ストリームに内に存在しても復号可能な装置を仮定しているため、メモリ部 104~106や復号部 108~110は音声用、動画像用、オブジェクト記述データ用に夫々複数用意されているものとする。

【0019】そして、復号部 108~110においてそれぞれ復号された音声オブジェクト、動画像オブジェクト、オブジェクト記述データは、シーン記述復号部 107で復号されたシーン記述情報データに基づいて、シーン合成部 112にて合成/グラフィック処理が行われる。このようにして得られた最終的なデータ列はディスプレイやプリンタ装置といった出力機器 113に供給されて可視化されることになる。

【0020】ここで、音声或いは動画像などのシーンを構成する個々のオブジェクトデータに対して、著作権などの保護のために再生を実行させたり、再生を停止させたりする制御が必要となる場合には、IPMP (Intellectual Property Management and Protection) 情報を用いて制御を行う。この IPMP 情報は、受信データの構成要素である IPMP データにて伝送される。IPMP 制御部 111は、分離部 102からの IPMP データに含まれる IPMP 情報に基づき、必要に応じて制御ポイントにおいてストリームを遮断したり、復号部 108~110にアクセスして、復号動作の停止を命令する。このため IPMP 制御部 111が、IPMP 情報等に基づいてデータの視聴の権利が無いと判断した場合には、該データが復号されなくなるので、再生が行われなくなる。このような制御を行うことで著作権を有するデータの保護を行う。

【0021】この IPMP 情報は、図 2 に示すような IPMP ディスクリプタ、又は IPMP メッセージにて伝送されることになっている。しかし、図 2 から分かるように、規格によって決められているのは、IPMP 情報が記述されるべき領域のみであり、実際に使用されるデータのシンタックスについては何ら規定されていない。そのため、オブジェクトデータを提供する企業毎に異なる IPMP 情報が存在し、それらの間には互換性がない可能性がある。このような場合には、自分のデータ処理装置が処理できる IPMP データの型と、再生しようとするオブジェクトデータの IPMP データの型とが一致していないと、所望するオブジェクトデータの再生

が出来ないばかりか、場合によってはデータ処理装置が暴走する危険性もある。このような事態を回避するために以下のような方式が提案されている。

【0022】この方式によると、ユーザが再生しようと所望するオブジェクトデータの IPMP データの型を、ユーザ自身のデータ処理装置が処理できる IPMP データの型に変換するデータ変換装置をデータ処理装置とオブジェクトデータの供給源 (コンテンツサーバ) との間に置き、データの送受信は、このデータ変換装置を介して行うというものである。

【0023】この仕組みを図 3 に基づいて説明する。コンテンツサーバ 1 (301) に格納してあるオブジェクトデータの IPMP データの型は "1" であるとし、コンテンツサーバ 2 (302) に格納してあるオブジェクトデータの IPMP データの型は "2" であるとする。一方、データ処理装置 303 が処理できる IPMP データの型は "1" であるとする。この IPMP データの型は、上記 "1", "2" の型の他にも複数存在することが考えられる。ここでは、データの型 "1" から "2" への変換の場合について説明する。

【0024】このデータ処理装置 303 がコンテンツサーバ 1 (301) のオブジェクトデータ (オブジェクトデータの IPMP データの型は "1") をネットワーク経由で受信した後に再生するのは、IPMP データの型が一致するので可能である。しかし、このデータ処理装置 303 がコンテンツサーバ 2 (302) のオブジェクトデータ (オブジェクトデータの IPMP データの型は "2") をネットワーク経由で受信して再生することは、IPMP データの型が一致しないため、不可能である。そこで、このような場合には、データ変換装置 304 においてコンテンツサーバ 2 (302) からの IPMP データを変換してからデータ処理装置 303 に送信する。ここでは、IPMP データの型が "2" から "1" への変換が行われる。

【0025】ここで著作権保護のために、オブジェクトデータに対してオブジェクトデータを提供する企業独自の暗号化をはじめとする様々なデータ変換が施されている場合は、それらのデータ変換の逆変換を行ってオリジナルの状態に戻してから、再度ユーザの持つデータ処理装置 303 が処理できるようなデータに変換する。このような処理を行うことで、ユーザの持つデータ処理装置 303 が処理できる IPMP データの型がどのようなものでも、またユーザが再生を所望するオブジェクトデータの IPMP データの型がどのようなものであっても、データを再生することが可能になる。

【0026】次に本実施の形態に係るコンテンツサーバ 1, 2 (301, 302)、データ変換装置 304、データ処理装置 (ユーザ端末) 303、証明書発行装置 (認証装置) 305 を含むデータ配信システムにおける各装置間のデータの流れを説明する。

【0027】図 4 は、本発明の実施の形態に係るデータ

配信システムにおける各装置間のデータの流れを説明する図である（課金装置無しのシステム）。

【0028】ここで図3と同様に、データ処理装置303は、IPMPデータの型が“1”のデータを処理及び表示することができ、コンテンツサーバ1(301)には、IPMPデータの型が“1”のデータであるコンテンツデータ1が蓄積されており、コンテンツサーバ2(302)には、IPMPデータの型が“2”のデータであるコンテンツデータ2が蓄積されている。データ変換装置304は、IPMPデータの型が“1”のコンテンツデータ1をIPMPデータの型が“2”のデータ（コンテンツデータ1-ex2）に変換でき、その逆のIPMPデータの型が“2”のコンテンツデータ2をIPMPデータの型が“1”のデータ（コンテンツデータ2-ex1）に変換することもできる。更に、コンテンツデータ1に対して「方式1」により暗号化処理等のデータ変換が施されており、コンテンツデータ2に対して「方式2」により暗号化処理等のデータ変換が施されている場合に、これらの方式の変換、即ち、「方式1」による処理が施されているコンテンツデータ1を逆変換して元のオリジナルの状態に戻してから「方式2」によるデータ変換を施すといったデータ変換を行う。証明書発行装置305は、各装置からの証明書発行要求を受けると、その要求してきた装置に対して証明書を発行するかどうかを判断し、発行の許可を決定した装置に対して証明書を発行して送出する。

【0029】以下、データ処理装置303が所望のコンテンツを得るまでの過程について記述する。

【0030】予め各装置は、証明書発行装置305に証明書発行要求を送出して証明書を発行してもらい、その証明書を自装置に保持しておく。データ処理装置303は、取得するコンテンツがユーザによって決められると、そのコンテンツが存在するコンテンツサーバに対して、そのサーバ内に複数存在するコンテンツから取得したいコンテンツを特定するために必要な番号を特定するコンテンツIDと、上記で得た証明書と、自分が処理できるIPMPの型を含むデータをリクエスト信号として送信する。ここでデータ処理装置303が処理できるIPMPデータの型は“1”であるとする。

【0031】以下、各場合について説明する。

(1)：リクエスト信号を送信した先のコンテンツサーバが持つコンテンツデータのIPMPデータの型が“1”である場合（コンテンツサーバ1(301)の場合）

(1-1)：コンテンツサーバ1(301)は、証明書発行装置305から送られた証明書をチェックしてから、そのデータを要求しているデータ処理装置303が処理できるIPMPの型が“1”であることを確認する。このチェックは該証明書が改竄されていないか、有効期間内であるか、本当に証明書発行装置305によって発行されたものであるかどうか等について検証する。このチェック、IPMPの型の確認が問題なく終了すると、次はコ

ンテンツサーバ1(301)がデータ処理装置303に対して、自装置の証明書を含むデータを肯定応答信号として送信する。また、この証明書チェックにおいて、この証明書の不正が検出された場合には、否定応答信号をデータ処理装置303に対して送信する（図4の401で示す）。

【0032】この否定応答信号を受信したデータ処理装置303は、認証に失敗した旨のメッセージを表示して処理を終了する。

10 【0033】一方、肯定応答信号を受信したデータ処理装置303は、送られてきたコンテンツサーバ1(301)の証明書をチェックし、該チェックが問題無く終了したら、今度はコンテンツIDで構成されるリクエスト信号をコンテンツサーバ1(301)に対して送る。コンテンツサーバ1(301)は、このリクエスト信号を受信すると、その要求されたコンテンツIDに対応するコンテンツデータを、そのデータ処理装置303に送信する（図の401）。このようにしてデータ処理装置303に送られたコンテンツデータに、IPMPデータの型“1”に対応する暗号処理等のデータ変換処理を施すことにより、伝送路上等でデータが盗聴された場合でも、著作権を有するコンテンツデータの保護が実現できる。

【0034】このコンテンツデータを受信したデータ処理装置303は、自装置に組み込まれているIPMPシステムを用いてIPMPデータの型が“1”のデータを処理して、ディスプレイやスピーカ等に出力する。また受信したコンテンツデータにIPMPデータの型“1”に対応する暗号処理等のデータ変換が施されている場合にも上記と同様に、自装置に組み込まれているIPMPシステムを用いて逆変換及びデータ処理を行いディスプレイやスピーカ等に出力する。

【0035】次に、コンテンツデータに暗号処理がなされている場合の鍵データの流れについて説明する。

【0036】このような暗号化処理が行われている場合、コンテンツサーバ1(301)からの鍵データはIPMPデータの中に含まれるか、或いは別途何らかのルートでデータ処理装置に送られる。

(2)：リクエスト信号を送信した先のコンテンツサーバが持つコンテンツデータのIPMPデータの型が“2”である場合（コンテンツサーバ2(302)の場合）

(2-1)：コンテンツサーバ2(302)は、送られた証明書をチェックしてから、データの要求をしているデータ処理装置303が処理できるIPMPの型を確認する。ここでは、データ処理装置303で処理できるIPMPの型が“1”であり、コンテンツサーバ2(302)の持つコンテンツデータのIPMPデータの型が“2”であるので、コンテンツサーバ2(302)は、データ処理装置303に対して、自装置の証明書を含むデータと、データ変換装置304のロケーション情報（IPアドレス）を肯定応答信号として送信する（図4の402で示す）。

(2-2) : データ処理装置 303 は、この送られてきたコンテンツサーバ 2 (302) の証明書をチェックし、このチェックが問題無く終了したら、指定されたロケーション情報に基づき、データ変換装置 304 に対して所望するコンテンツ ID と、該コンテンツ ID のコンテンツが存在するコンテンツサーバのロケーション情報 (IP アドレス) と、自装置の証明書と、自分が処理できる IPMP の型とで構成されるデータをリクエスト信号として送信する (図 4 の 403 で示す)。

(2-3) : データ変換装置 304 は、この送られてきたデータ処理装置 303 の証明書をチェックし、このチェックが問題無く終了したら、自装置の証明書を含む肯定応答信号をデータ処理装置 303 に対して送る (図 4 の 405 で示す) と同時に、コンテンツサーバ 2 (302) に対してコンテンツ ID と自装置の証明書とで構成されるデータをリクエスト信号として送信する (図 4 の 404 で示す)。

【0037】一方、データ変換装置 304 は、このチェックにおいて不正が検出された場合には、否定応答信号をデータ処理装置 303 に対して送信する (405)。この否定応答信号を受信したデータ処理装置 303 は、認証に失敗した旨のメッセージを表示して処理を終了する。

【0038】また、(2-3) で送信されたデータ変換装置 304 の証明書を含む肯定応答信号を受信したデータ処理装置 303 は、この証明書のチェックを行う。このチェックにおいて不正が検出された場合には、認証に失敗した旨のメッセージを表示して処理を終了する。

【0039】コンテンツサーバ 2 (302) は、出た変換装置 304 から受信したリクエスト信号に含まれるデータ変換装置 304 の証明書をチェックしてから、その要求されたコンテンツ ID に対応するコンテンツデータ 2 をデータ変換装置 304 に送信する (404)。

【0040】一方、コンテンツサーバ 2 (302) における証明書のチェックにおいて不正が検出された場合には、否定応答信号をデータ変換装置 304 に対して送信する (404)。この否定応答信号を受信したデータ変換装置 304 は、データ処理装置 303 に対して否定応答信号を送信する (405)。

【0041】ここで、データ変換装置 304 がコンテンツサーバ 2 (302) から受信したコンテンツデータ 2 の IPMP データの型は "2" であり、この実施の形態に係るデータ処理装置 303 が処理可能なデータの型ではない。従って、このコンテンツデータ 2 を受信したデータ変換装置 304 は、このデータ処理装置 303 が処理できるようにコンテンツデータ 2 をデータ変換する。

【0042】具体的には、コンテンツデータ 2 の IPMP データの型は "2" であるので、該 IPMP データの型を "2" から "1" に変換する処理を行う。ここで、コンテンツデータ 2 に IPMP データの型 "2" に対応する暗号

処理等のデータ変換が施されている場合には、この変換の逆変換を行うことでコンテンツデータを一旦元の状態に戻し、今度は IPMP データの型 "1" に対応する暗号処理等のデータ変換を行う。これらの処理によりコンテンツデータ 2 は、データ処理装置 303 で処理できるコンテンツデータ (2-ex1) に変換される。

(2-4) : データ変換装置 304 は、このコンテンツデータ (2-ex1) をデータ処理装置 303 に送信する (図 4 の 405)。このコンテンツデータ (2-ex1) を受信したデータ処理装置 303 は、自装置に組み込まれている IPMP システムを用いて上記データを処理して、ディスプレイやスピーカ等に出力する。

【0043】また、受信したコンテンツデータに IPMP データの型 "1" に対応する暗号処理等のデータ変換が施されている場合も、自装置に組み込まれている IPMP システムを用いて逆変換及びデータ処理を行ってディスプレイやスピーカ等に出力する。

【0044】ここで、コンテンツデータに暗号処理がなされている場合の鍵データの流れについて説明する。

【0045】このような暗号化処理が行われている場合、コンテンツサーバ 2 (302) からの鍵データは、IPMP データの中に含まれる形でデータ変換装置 304 に送信された後に、データ変換装置 304 にてデータ処理装置 303 が処理を行える IPMP データの型に変換されてからデータ処理装置 303 に送られるか、又は別途何らかのルートでデータ処理装置 303 に送られる。

【0046】図 5 は、本発明の実施の形態に係る配信システムにおける各装置間のデータの流れを示す図である (課金装置 501 有りの場合のシステム)。

【0047】データ処理装置 303 は、IPMP データの型が "1" のデータを処理及び表示することができ、コンテンツサーバ 1 (301) には、IPMP データの型が "1" のデータであるコンテンツデータ 1 が蓄積されており、コンテンツサーバ 2 (302) には、IPMP データの型が "2" のデータであるコンテンツデータ 2 が蓄積されている。データ変換装置 304 は、IPMP データの型が "1" のコンテンツデータ 1 を、IPMP データの型が "2" のデータ (コンテンツデータ (1-ex2)) に変換でき、その逆の IPMP データの型が "2" のコンテンツデータ 2 を、IPMP データの型が "1" のデータ (コンテンツデータ (2-ex1)) に変換することもできる。更に、コンテンツデータ 1 に対して「方式 1」により暗号化処理等のデータ変換が施されており、またコンテンツデータ 2 に対して「方式 2」により暗号化処理等のデータ変換が施されている場合に、これらの方式の間の変換、即ち、「方式 1」による処理が施されているコンテンツデータ 1 を逆変換して元のオリジナルの状態に戻してから「方式 2」によるデータ変換を施すといったデータ変換を行う。

【0048】課金装置 501 は、データ変換装置 304

又はコンテンツサーバ 1 (301) から、このサーバ 1 やデータ変換装置 304 がデータ処理装置 303 に送付したコンテンツデータの対価に関するデータ (課金/決済を行うために必要となるデータ) を受け取り、ユーザ毎の課金データを生成する。この課金装置 501 は、外部の金融機関等と接続されており、この課金装置 501 で生成した課金データがこれらの機関に送られる。証明書発行装置 305 は、各装置からの証明書発行要求を受けると、その要求してきた装置に対して証明書を発行するかどうかを判断し、発行の許可を決定した装置に対しては証明書を発行/送出する。

【0049】以下、データ処理装置 303 が所望のコンテンツを得るまでの過程について記述する。

【0050】予め各装置は、証明書発行装置 305 に証明書発行要求を送出し、証明書を発行してもらい自装置に保持しておく。データ処理装置 303 は、取得するコンテンツがユーザによって決められると、そのコンテンツが存在するコンテンツサーバに対して、そのコンテンツサーバ内に複数存在するコンテンツから取得したいコンテンツデータを特定するために必要な番号であるコンテンツ ID と、上記で得た証明書と、自分が処理できる IPMP の型とで構成されるデータをリクエスト信号として送信する。ここでデータ処理装置 303 が処理できる IPMP データの型は "1" であるとする。

(1) : リクエスト信号を送信した先のコンテンツサーバが持つコンテンツデータの IPMP データの型が "1" である場合 (コンテンツサーバ 1 (301) の場合)

(1-1) : コンテンツサーバ 1 (301) は、送られた証明書をチェックしてから、そのコンテンツデータを要求しているデータ処理装置 303 が処理できる IPMP の型が "1" であることを確認する。このチェックは該証明書が改竄されていないか、有効期間内であるか、本当に証明書発行装置 305 によって発行されたものであるかどうか等について検証する。このチェック、IPMP の型の確認が問題無く終了すると、次にコンテンツサーバ 1 (301) は、そのデータ処理装置 303 に対して、自装置の証明書を含むデータを肯定応答信号として送信する (図 5 の 501)。尚、この証明書チェックにおいて、この証明書の不正が検出された場合には、否定応答信号をデータ処理装置 303 に対して送信する。

【0051】コンテンツサーバ 1 (301) から肯定応答信号を受信したデータ処理装置 303 は、上記と同様に、送られてきたコンテンツサーバ 1 (301) の証明書をチェックし、このチェックが問題無く終了したら、今度はコンテンツ ID で構成されるリクエスト信号をコンテンツサーバ 1 (301) に対して送る。コンテンツサーバ 1 (301) は、このリクエスト信号を受信すると、要求されたコンテンツ ID に対応するデータをデータ処理装置 303 に送信すると同時に、課金/決済を行うために必要となるデータを生成する。

【0052】一方、否定応答信号を受信したデータ処理装置 303 は、認証に失敗した旨のメッセージを表示して処理を終了する。

【0053】コンテンツサーバ 1 (301) において生成される課金/決済を行うために必要となるデータの構成例を図 6 に示す。

【0054】このデータはユーザ名、ユーザ ID、送信したコンテンツ ID、送信した日時等で構成される。

(1-2) : このデータが課金装置 501 に送られて (図 5 の 502)、そこで課金データが生成される。

【0055】ここでデータ処理装置 303 に送られたコンテンツデータに、IPMP データの型 "1" に対応する暗号処理等のデータ変換を施すことにより、伝送路上等でデータが盗聴された場合でも著作権を有するコンテンツデータの保護が実現できる。このコンテンツデータを受信したデータ処理装置 303 は、自装置に組み込まれている IPMP システムを用いて IPMP データの型が "1" のデータを処理し、ディスプレイやスピーカ等に出力する。

【0056】また、受信したコンテンツデータに IPMP データの型 "1" に対応する暗号処理等のデータ変換が施されている場合にも上記と同様に、自装置に組み込まれている IPMP システムを用いて、逆変換及びデータ処理を行ってディスプレイやスピーカ等に出力する。

【0057】ここで、コンテンツデータに暗号処理がなされている場合の鍵データの流れについて説明する。

【0058】このような暗号化処理が行われている場合、コンテンツサーバ 1 (301) からの鍵データは IPMP データの中に含まれるか、或いは別途何らかのルートでデータ処理装置 303 に送られる。この際、コンテンツサーバ 1 (301) は、鍵データを送信した記録として、図 6 の「鍵データの送信」欄に鍵データを格納する。このコンテンツデータに暗号化等のデータ変換が施されていない場合には、このコンテンツデータは無料と考えて課金の対象にしない。一方、暗号化等のデータ変換が施されている場合には、このコンテンツデータを有料と考えて課金を行うといったことが考えられる。このような場合には、この鍵データの存在するブロックのみを課金/決済を行うために必要となるデータとすることができ

(2) : リクエスト信号を送信した先のコンテンツサーバが持つコンテンツデータの IPMP データの型が "2" である場合 (コンテンツサーバ 2 (302) の場合)

(2-1) : コンテンツサーバ 2 (302) は、送られた証明書をチェックしてから、データを要求をしているデータ処理装置 303 が処理できる IPMP の型を確認する。ここでは、データ処理装置 303 で処理できる IPMP の型が "1" であり、コンテンツサーバ 2 (302) の持つコンテンツデータの IPMP データの型が "2" であるので、コンテンツサーバ 2 (302) は、データ処理装置 3

03に対して、自装置の証明書を含むデータと、データ変換装置304のロケーション情報(IPアドレス)を肯定応答信号として送信する(図5の503)。

(2-2):データ処理装置303は、送られてきたコンテンツサーバ2(302)の証明書をチェックし、このチェックが問題無く終了したら、指定されたロケーション情報に基づいて、データ変換装置304に対して所望するコンテンツIDと、そのコンテンツIDのコンテンツが存在するコンテンツサーバのロケーション情報(IPアドレス)と、自装置の証明書と、自分が処理できるIPMPの型とで構成されるデータを、リクエスト信号としてデータ変換装置304に送信する(図5の504)。

(2-3):データ変換装置304は、その送られてきたデータ処理装置303の証明書をチェックし、該チェックが問題無く終了したら、自装置の証明書を含む肯定応答信号をデータ処理装置303に対して送ると(505)同時に、コンテンツサーバ2(302)に対して、コンテンツIDと自装置の証明書とで構成されるデータをリクエスト信号として送信する(506)。コンテンツサーバ2(302)は、その受信したデータ変換装置304の証明書をチェックしてから、リクエスト信号で要求されたコンテンツIDに対応するコンテンツデータ2をデータ変換装置304に送信する(506)。そして、これと同時に、課金を行うために必要となるデータを生成する。このデータは上記図6と同様のデータである。ここで、データ変換装置304がコンテンツサーバ2(302)から受信したコンテンツデータ2のIPMPデータの型は"2"であり、このコンテンツデータ2を受信したデータ変換装置304は、データ処理装置303がコンテンツデータ2を処理可能になるようにデータの変換を行う。

【0059】一方、データ変換装置304における上記証明書をチェックで不正が検出された場合には、否定応答信号をデータ処理装置303に対して送信する(505)。この否定応答信号を受信したデータ処理装置303は、認証に失敗した旨のメッセージを表示して処理を終了する。

【0060】またデータ変換装置304から、証明書を含む肯定応答信号を受信したデータ処理装置303は、該証明書のチェックを行う。このチェックにおいて不正が検出された場合には、その認証に失敗した旨のメッセージを表示して処理を終了する。

【0061】また一方、このチェックにおいて不正が検出された場合には、否定応答信号をデータ変換装置304に対して送信する。この否定応答信号を受信したデータ変換装置304は、データ処理装置303に対して否定応答信号を送信する。

【0062】チェックが問題ない場合には、データ変換装置304は、コンテンツデータ2のIPMPデータの

型が"2"であるので、このIPMPデータの型を"2"から"1"に変換する処理を行う。ここで、コンテンツデータ2にIPMPデータの型"2"に対応する暗号処理等のデータ変換が施されている場合には、該変換の逆変換を行うことでコンテンツデータを元の状態に戻し、その後、IPMPデータの型"1"に対応する暗号処理等のデータ変換を行う。これらの処理によりコンテンツデータ2は、データ処理装置303が処理できるコンテンツデータ(2-ex1)に変換される。

10 (2-4):課金を行うために必要となるデータが、コンテンツサーバ2(302)から課金装置501に送られ課金データが生成される(図5の508)。

(2-5):データ変換装置304は、変換したコンテンツデータ(2-ex1)をデータ処理装置303に送信する(505)。更に、データ変換を行ったことに対する料金を計算するためのデータを生成する。

【0063】このデータの構成例を図7に示す。

20 【0064】このデータは、ユーザ名、ユーザID、変換したコンテンツID(送信コンテンツID)、送信した日時、変換したデータ量、どんな型のIPMPデータに変換したかを示す情報等で構成される。

(2-6):このデータがデータ変換装置304から課金装置501に送られて課金データが生成される(507)。

30 【0065】又、データ変換装置304からコンテンツデータ(2-ex1)を受信したデータ処理装置303は、自装置に組み込まれているIPMPシステムを用いて上記データを処理し、ディスプレイやスピーカ等に出力する。また、受信したコンテンツデータにIPMPデータの型"1"に対応する暗号処理等のデータ変換が施されている場合にも、自装置に組み込まれているIPMPシステムを用いて逆変換及びデータ処理を行ってディスプレイやスピーカ等に出力する。

【0066】次に、コンテンツデータに暗号処理がなされている場合の鍵データの流れについて説明する。

40 【0067】このような暗号化処理が行われている場合、コンテンツサーバ2(302)からの鍵データは、IPMPデータの中に含まれる形でデータ変換装置304に送信された後、このデータ変換装置304において、データ処理装置303が処理を行えるようなIPMPデータの型に変換してからデータ処理装置303に送られるか、または別途何らかのルートでデータ処理装置303に送られる。データ変換装置303を経由して鍵データが送られた場合、上述の場合と同様に、データ変換装置304は、鍵データを送信した記録として図7の「鍵データの送信」欄に鍵データを格納する。

50 【0068】ここでは、図4および図5に基づいて各装置間のデータの流れについて説明したが、このデータの流れは一つの例であり、他にも様々なデータの流れが存在する。しかし他のデータの流れにおいても、データ処

理装置 303 が処理できない IPMP データを持つコンテンツデータを要求した場合には、そのコンテンツデータはデータ変換装置 304 を経由して、要求元であるデータ処理装置 303 に入力されて、データ処理及び表示が行われる。また課金を行うために必要なデータが、データ変換装置 304 やコンテンツサーバから課金装置 501 に入力されるという点は、上記実施の形態と同様である。

【0069】以下、本実施の形態に係る各装置の動作、特にデータ処理装置 303 の処理の一例について図 8 のフローチャートを用いて説明する。

【0070】図 8 は、本実施の形態に係る配信システムにおいて、データ処理装置 303 がデータ変換装置 304、コンテンツサーバからのデータを受信し、そのデータを再生する際の処理を説明するためのフローチャートである。

【0071】図 8 において、まずステップ S801 で、証明書発行装置 305 に証明書発行要求を送出して証明書を発行／送信してもらい、その証明書を自装置に保持する。以後の認証処理では、この保持している証明書を

【0072】次にステップ S802 に進み、このデータ処理装置 303 のユーザにより、再生したいコンテンツが決定されると、そのコンテンツを取得するために必要な情報がデータ処理装置 303 に入力される。これによりステップ S803 で、データ処理装置 303 から、コンテンツサーバに対して、そのサーバ内に複数存在するコンテンツから所望のコンテンツを特定するために必要な番号であるコンテンツ ID と、証明書発行装置 305 からの証明書と、自装置が処理できる IPMP の型とで

【0073】次にステップ S804 に進み、そのコンテンツサーバからの応答が肯定応答信号であるか、否定応答信号であるかを判断する。応答が否定応答信号である場合はステップ S805 に進む。ここで、受信した応答が否定応答信号であるということは、自装置の証明書が接続先のコンテンツサーバにおいて認証されなかったことを意味するので、「証明書がコンテンツサーバにて認証されませんでした」とのメッセージを表示部（不図示）に表示して処理を終了する。

【0074】一方ステップ S804 で、応答が肯定応答信号である場合はステップ S806 に進み、コンテンツサーバの証明書のチェックを行う。このチェックは、その証明書が改竄されていないか、有効期間内であるか、又、本当に証明書発行装置 305 によって発行されたものであるかどうか等について検証するものである。この検証の結果、証明書が正当でないと判断した場合にはステップ S807 に進み、コンテンツサーバの証明書を認証できなかったことを意味する「コンテンツサーバの証明書を認証することが出来ませんでした」とのメッセー

ジを表示して処理を終了する。

【0075】一方ステップ S806 で、チェックにより証明書が正当であると判断した場合はステップ S808 に進み、肯定応答信号の中のロケーション情報（データ変換装置 304 の IP アドレス等）があるか無いかが検証される。ここで、ロケーション情報があるということは、接続先のコンテンツサーバの持つコンテンツデータの IPMP データの型が自装置では処理出来ないことを意味し、ロケーション情報が無いということは、接続先のコンテンツサーバの持つコンテンツデータの IPMP データの型が自装置で処理出来ることを意味する。従って、ロケーション情報が無い場合はステップ S809 に進み、コンテンツ ID で構成されるリクエスト信号をコンテンツサーバに対して送る。次にステップ S810 に進み、所望するコンテンツデータを受信して、自装置に組み込まれている IPMP システムを用いて、そのコンテンツデータを処理し、ディスプレイやスピーカ等に出して処理を終了する。

【0076】一方、ステップ S808 で、ロケーション情報が有る場合、即ち、接続先のコンテンツサーバの持つコンテンツデータの IPMP データの型が自装置では処理出来ない場合にはステップ S811 に進み、そのロケーション情報に基づき、所望するコンテンツ ID と、そのコンテンツ ID のコンテンツの存在するコンテンツサーバのロケーション情報（IP アドレス）と、自装置の証明書と、自分が処理できる IPMP の型とで構成されるデータを、データ変換装置 304 に対してリクエスト信号として送信する。次にステップ S812 に進み、データ変換装置 304 からの応答が肯定応答信号か、否定応答信号であるかを判断する。応答が否定応答信号である場合にはステップ S813 に進む。ここで、受信した応答が否定応答信号であるということは、自装置の証明書が接続先のデータ変換装置 304 において認証されなかったか、又はコンテンツサーバにおいてデータ変換装置 304 の証明書が認証されなかったことを意味するので、「証明書が認証されませんでした」とのメッセージを表示して処理を終了する。

【0077】一方、ステップ S812 で、応答が肯定応答信号である場合にはステップ S814 に進み、データ変換装置 304 の証明書のチェックを行う。このチェックは、その証明書が改竄されていないか、有効期間内であるか、また本当に証明書発行装置 305 によって発行されたものであるかどうか等について検証するものである。この検証の結果、その証明書が正当でないと判断した場合にはステップ S815 に進み、データ変換装置 304 の証明書を認証できなかったことを意味する「データ変換装置の証明書を認証することが出来ませんでした」とのメッセージを表示して処理を終了する。

【0078】またステップ S814 で、データ変換装置 304 の証明書のチェックにより正当であると判断した

場合にはステップS816に進み、要求しているコンテンツデータを受信して、自装置に組み込まれているIPMPシステムを用いて、そのコンテンツデータを処理し、ディスプレイやスピーカ等に出力して処理を終了する。

【0079】次に、上記の認証処理で用いられる証明書の発行処理を行う証明書発行装置305の処理の一例について図9のフローチャートを用いて説明する。

【0080】図9は、証明書発行装置305がデータ処理装置303、データ変換装置304、コンテンツサーバ301、302、課金装置501からの証明書発行要求を受信し、各証明書の発行を行う際の処理を説明するためのフローチャートである。

【0081】図9において、まずステップS901で、データ処理装置303、データ変換装置304、コンテンツサーバ301、302、課金装置501から証明書発行要求をネットワーク経由で受信する。この証明書発行要求は、要求者の識別名、自装置に関する公開情報、これらのデータが伝送路上で改竄されていないことを証明するためのデータ等で構成される。

【0082】この要求を受信するとステップS902に進み、各装置から受信した証明書発行要求を解析する。具体的には、データの改竄を証明するデータを用いて、要求者の識別名や自装置に関する公開情報等が改竄されていないかどうか、証明書を登録してあるデータベースに既に登録されていないかどうか、一度発行した証明書を無効にするためのデータベースに登録されていないかどうか、場合によっては識別名が示す組織、会社が実際に存在するかどうかといったことに関する各種チェックを行う。ここで、この証明書発行に際して、そのチェックを厳格に行うか、或いは簡易に行うのかを設定できるような仕組みが備わっていることが望ましい。

【0083】この解析が終了するとステップS903に進み、ステップS902における解析結果に基づいて、各装置に対する証明書を発行するかどうかを判断する。ここで発行を行わないと判断した場合にステップS907に進み、証明書が発行できなかったこと旨のメッセージを証明書発行要求を送信してきた発行元の装置に送信して、処理を終了する。

【0084】一方ステップS903で、発行を行うと判断した場合にはステップS904に進み、その証明書発行要求の内容に基づいて発行処理を行う。ここで発行される証明書は、証明書のバージョン番号、シリアル番号、証明書を発行した装置名、有効期限、ユーザの公開情報、該証明書が伝送路上で改竄されていないことを証明するためのデータ等で構成される。次にステップS905に進み、ステップS904で発行した証明書を、その証明書発行要求を送信してきた各装置に送信する。次にステップS906に進み、上記ステップS904で発行した証明書を登録用データベースに登録し、同じ識別

名で2重の登録がなされないように管理する。なお、この登録用データベースは、証明書発行装置305の内部に設けられていても良く、或いは証明書発行装置305の外部にあって、ネットワーク等で接続された装置内に設けられていても良い。こうしてステップS906の登録処理が済めば処理終了となる。

【0085】尚、ここで、一度発行された証明書を何らかの理由により無効にしたい場合は、その証明書を所有している装置は証明書発行装置305に対して、証明書無効化要求を送信する。これにより証明書発行装置305は、無効となる証明書のみを含む無効データベースに、その要求された証明書を移動して登録する。このような処理を行うことで、その要求された証明書を無効とすることができる。

【0086】次に、コンテンツの対価に対する決済を行う課金装置501の処理の一例について図10のフローチャートを用いて説明する。

【0087】図10は、課金装置501がデータ変換装置303、コンテンツサーバ301、302からの課金/決済を行うためのデータを受信し、その受信したデータに基づいて行う決済処理を説明するためのフローチャートである。

【0088】図10において、まずステップS901で、データ変換装置304、コンテンツサーバ301、302から課金/決済を行うためのデータを受信する。このデータは前述の図6や図7で示されるものである。次にステップS1002に進み、ステップS1001で受信したデータを基にしてユーザ毎の課金データを生成する。次にステップS1003に進み、ステップS1002で生成した課金データをデータベースに登録して、ユーザ毎に管理する。なお、このデータベースは課金装置501の内部に存在してもよいし、この課金装置501の外部にあるネットワーク等で接続された装置に存在してもよい。

【0089】次にステップS1004に進み、課金データの送信時間であるかどうか判断される。これは例えば、金融機関は月末等の一定期間毎に決済処理を行っている。そのため、この課金データは生成される毎に送信する必要は必ずしも無い。そこである一定期間を予め決めておき、その時間が来たら一気に課金データを送信するようにする。ステップS1004で送信時間になった時はステップS1005に進み、そうでない時は送信時間がくるまで、このステップS1004を繰り返す。

【0090】ステップS1005では、ステップS1003で登録した課金データを、スケジュールに従って、対応する銀行やクレジット会社等の金融機関の処理装置に送信する。次にステップS1006に進み、送信した課金データに対する応答が肯定応答信号であるかどうか判断される。金融機関の処理装置は、課金データを確実に受信した場合には肯定応答信号を課金装置501に

対して送信し、一方、受信に失敗した場合には否定応答信号を送信するので、応答が肯定応答信号である場合には、課金装置 501 は、課金データが正常に受信されたと判断して処理を終了する。

【0091】一方、応答が否定応答信号である場合には、前回ステップ S1005 で送信した課金データが受信されていないと判断して再度ステップ S1005 に戻り、ステップ S1006 で肯定応答信号を受取るまで、このステップ S1005 の処理を繰り返す。

【0092】次に、コンテンツデータの変換を行うデータ変換装置 304 の処理の一例について図 11 のフローチャートを用いて説明する。

【0093】図 11 は、データ変換装置 304 がコンテンツサーバからのコンテンツデータを受信し、そのコンテンツデータをデータ処理装置 303 が処理できるようなデータに変換するための処理を説明するためのフローチャートである。なお、このデータ変換装置 304 が動作するのは、データ処理装置 303 が処理可能な IPMP データの型とユーザが所望するコンテンツデータの IPMP データの型とが異なる場合である。

【0094】図 11 において、まずステップ S1101 で、データ処理装置 303 が変換を所望するコンテンツ ID と、そのコンテンツ ID のコンテンツが存在するコンテンツサーバのロケーション情報（IP アドレス）と、データ処理装置 303 の証明書と、データ処理装置 303 が処理できる IPMP の型とを含むデータを、リクエスト信号としてデータ処理装置 303 から受信する。このリクエスト信号を受信するとステップ S1102 に進み、ステップ S1101 で受信したデータ処理装置 303 の証明書のチェックを行う。このチェックは、データ処理装置 303 の証明書が改竄されていないか、有効期間内であるか、また本当に証明書発行装置 305 によって発行されたものであるかどうか等について検証するものである。この検証の結果、その証明書が正当でないと判断した場合にはステップ S1103 に進み、証明書の検証に失敗したので、データ処理装置 303 に対して否定応答信号を送信して処理を終了する。

【0095】ステップ S1102 で、正当であると判断した場合はステップ S1104 に進み、上記ロケーション情報（IP アドレス）で示されているコンテンツサーバに対してコンテンツ ID とデータ変換装置 304 の証明書とを含むリクエスト信号を送信する。これと同時に、その要求元のデータ処理装置 303 に対して、そのデータ変換装置 304 の証明書を含む肯定応答信号を送信する。

【0096】次にステップ S1105 に進み、コンテンツサーバから受信したデータがコンテンツデータであるか、否定応答信号であるのかを判断する。ここで、受信したデータが否定応答信号である場合にはステップ S1106 に進む。ここでは、コンテンツサーバにおいてデ

ータ変換装置 304 の証明書が認証されなかったために否定応答信号を受信したのであるため、データ処理装置 303 に否定応答信号を送信して処理を終了する。

【0097】一方、ステップ S1105 で、コンテンツサーバから受信したデータがコンテンツデータである場合はステップ S1107 に進み、ステップ S1105 で受信したコンテンツデータを、ステップ S1101 でリクエスト信号を送信してきたデータ処理装置 303 が処理できるようなデータに変換する。次にステップ S1108 に進み、ステップ S1107 で変換したコンテンツデータを、そのデータ変換を要求してきたデータ処理装置 303 に送信する。そしてステップ S1109 に進み、データ変換を行ったことに対する料金を計算するために必要となるデータを生成する。このデータは図 7 に示されるものである。そして、生成したデータを課金装置 501 に対して送信して処理を終了する。

【0098】次に、コンテンツデータが格納されているコンテンツサーバの処理の一例について図 12 のフローチャートを用いて説明する。

【0099】図 12 は、本実施の形態に係るコンテンツサーバの行う処理を説明するためのフローチャートである。

【0100】図 12 において、まずステップ S1201 で、ユーザが取得したいコンテンツを特定するために必要な番号であるコンテンツ ID と、データ処理装置 303 の証明書と、データ処理装置 303 が処理できる IPMP の型とを含むデータを、リクエスト信号としてデータ処理装置 303 から受信する。このリクエスト信号を受信するとステップ S1202 に進み、ステップ S1201 で受信したデータ処理装置 303 の証明書のチェックを行う。このチェックは、その証明書が改竄されていないか、有効期間内であるか、また本当に証明書発行装置 305 によって発行されたものであるかどうか等について検証するものである。この検証の結果、証明書が正当でないと判断した場合にはステップ S1203 に進む。この場合は、リクエスト信号を発行したデータ処理装置 303 の証明書の検証に失敗したので、そのデータ処理装置 303 に対して否定応答信号を送信して処理を終了する。

【0101】一方、ステップ S1202 で、その証明書が正当であると判断した場合にはステップ S1204 に進み、ステップ S1201 で受信したリクエスト信号の発行元であるデータ処理装置 303 が処理できる IPMP の型と、コンテンツサーバ内にあるコンテンツデータの IPMP データの型とが一致するかどうかを判断する。一致していると判断された場合はステップ S1205 に進み、そのデータ処理装置 303 に対して、コンテンツサーバの証明書を含むデータを肯定応答信号として送信する。次にステップ S1206 に進み、データ処理装置 303 からコンテンツ ID で構成されるリクエスト

信号を受信する。そしてステップ S1207 に進み、ステップ S1206 で受信したリクエスト信号により要求されたコンテンツ ID に対応するデータをデータ処理装置 303 に送信する。これと同時に、コンテンツデータに対する課金を行うために必要となるデータを生成する。この生成したデータは図 6 に示されるものである。そしてステップ S1208 に進み、ステップ S1207 で生成したコンテンツデータに対する課金を行うために必要となるデータを課金装置 305 に送信して処理を終了する。

【0102】一方、ステップ S1204 で、IPMP の型が不一致と判断した場合にはステップ S1209 に進み、そのデータ処理装置 303 に対して、コンテンツサーバの証明書を含むデータとデータ変換装置 304 のロケーション情報（IP アドレス）とを含むデータを肯定応答信号として送信する。次にステップ S1210 に進み、コンテンツ ID とデータ変換装置 304 の証明書とを含むデータをリクエスト信号として、そのデータ処理装置 303 から受信する。これによりステップ S1211 に進み、ステップ S1210 で受信したデータ変換装置 304 の証明書のチェックを行う。このチェックは、その証明書が改竄されていないか、有効期間内であるか、また本当に証明書発行装置 305 によって発行されたものであるかどうか等について検証するものである。この検証の結果、証明書が正当でないと判断した場合にはステップ S1212 に進み、データ変換装置 304 に対して否定応答信号を送信して処理を終了する。

【0103】一方、ステップ S1211 で、正当であると判断した場合にはステップ S1213 に進み、ステップ S1210 で要求されたコンテンツ ID に対応するコンテンツデータをデータ変換装置 304 に送信する。これと同時に、コンテンツデータに対する課金を行うために必要となるデータを生成するこの該データは図 6 に示されるものである。次にステップ S1214 に進み、ステップ S1213 で生成したコンテンツデータに対する課金を行うために必要となるデータを課金装置 305 に送信して処理を終了する。

【0104】以上説明したように本実施の形態によれば、ユーザが使用するデータ処理装置からコンテンツサーバに対してコンテンツを要求して、そのコンテンツをユーザが取得できるとともに、そのコンテンツが自装置で処理できないデータの場合には、データ変換装置を使用してデータ変換を行い、その変換されたデータを受取ることにより、自装置の有していない方式で暗号化されたデータでも受信して再生できる。

【0105】更に、この構成に、証明書発行装置から発行された証明書による認証機能を付加することにより、認証された装置間でのデータの交換を行うことができる。

【0106】更に本実施の形態に係る特徴的な構成とし

て、コンテンツサーバ、データ変換装置は、ユーザからの要求に応じてコンテンツの提供、データ変換を実行すると、課金装置 501 により、それに伴う課金データを生成して、データ変換装置 303、コンテンツサーバ 301、302 からの課金/決済を行うことができる。これによりそのコンテンツの著作権者は、そのコンテンツの視聴を許可している人にだけそのコンテンツを提供でき、かつそのコンテンツを提供することによる報酬（課金）を自動的に得られるので、安心してコンテンツを提供することができる。

【0107】本発明は一つの機器（例えば複写機、ファクシミリ）からなる装置に適用しても、複数の機器（例えばホストコンピュータ、インタフェース機器、リーダ、プリンタ等）から構成されるシステムに適用してもよい。

【0108】また、前述した実施形態の機能を実現する様に各種のデバイスを動作させるために、該各種デバイスと接続された装置あるいはシステム内のコンピュータに、前記、実施形態を実現するためのソフトウェアのプログラムを供給し、そのシステムあるいは装置のコンピュータ（CPU、MPU）を格納させたプログラムに従って前記各種デバイスを動作させることによって実施したものも本発明の範疇に含まれる。

【0109】またこの場合、前記ソフトウェアのプログラム自体が前述した実施形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、例えばプログラムコードを格納した記憶媒体は本発明を構成する。

【0110】かかるプログラムコードを格納する記憶媒体としては例えばフロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、DVD-ROM、不揮発性のメモ리카ード等を用いることができる。

【0111】またコンピュータが、供給されたプログラムコードを実行することにより、前述の実施形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働している OS（オペレーティングシステム）、あるいは他のアプリケーションソフト等と共同して前述の実施形態の機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることは言うまでもない。

【0112】さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその拡張機能ボードや機能拡張ユニットに備わる CPU 等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も本発明の実施の形態に含まれることは言うまでもない。

【0113】以上説明したように本実施の形態によれ

ば、データ変換システム及びIPMPシステムと連携したユーザ認証、課金システムが構築できる。その結果、ネットワークを使用したコンテンツ配信サービスが現実的なものとなる。

【0114】

【発明の効果】以上説明したように本発明によれば、ユーザの認証に加えて、そのユーザによるコンテンツデータの取得及びデータ変換に伴う課金を自動的に行うことができる。

【0115】又本発明によれば、視聴を許可されたユーザだけがそのコンテンツデータを使用でき、かつ自動的に、そのユーザによるコンテンツデータの使用料を課金できるという効果がある。

【図面の簡単な説明】

【図1】本発明の実施の形態に係るデータ処理装置の概略構成を示すブロック図である。

【図2】本発明に係るIPMPデータのデータ構造を示す図である。

【図3】一般的な配信システムの全体構造の一例を示す図である。

【図4】本発明の実施の形態に係るデータ配信システム（課金装置無し）における各装置間のデータの流れを説明する図である。

【図5】本発明の実施の形態に係るデータ配信システム（課金装置あり）における各装置間のデータの流れを説明する図である。

【図6】本実施の形態に係る課金／決済を行うために必要となるデータの一例を示す図である。

【図7】本実施の形態に係る課金／決済を行うために必要となるデータの一例を示す図である。

【図8】本発明の実施の形態に係るデータ処理装置の動作を説明するためのフローチャートである。

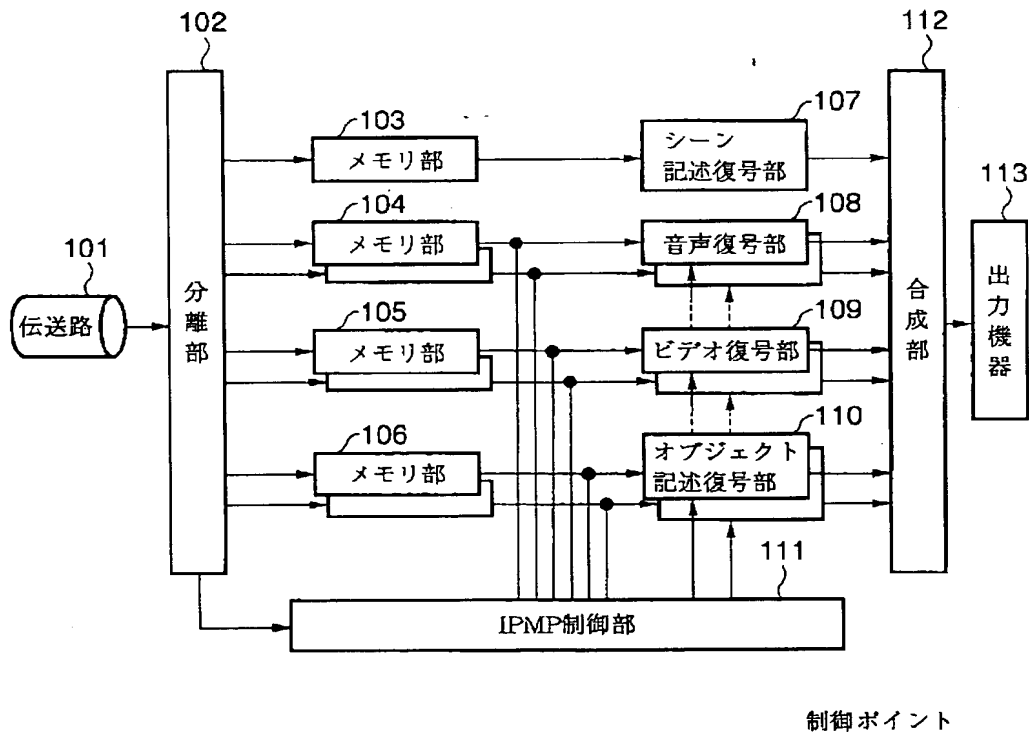
【図9】本発明の実施の形態に係る証明書発行装置の動作を説明するためのフローチャートである。

【図10】本発明の実施の形態に係る課金装置の動作を説明するためのフローチャートである。

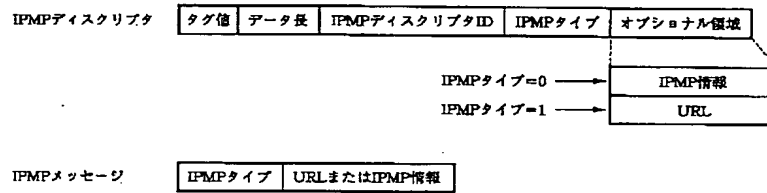
【図11】本発明の実施の形態に係るデータ変換装置の動作を説明するためのフローチャートである。

【図12】本発明の実施の形態に係るコンテンツサーバの動作を説明するためのフローチャートである。

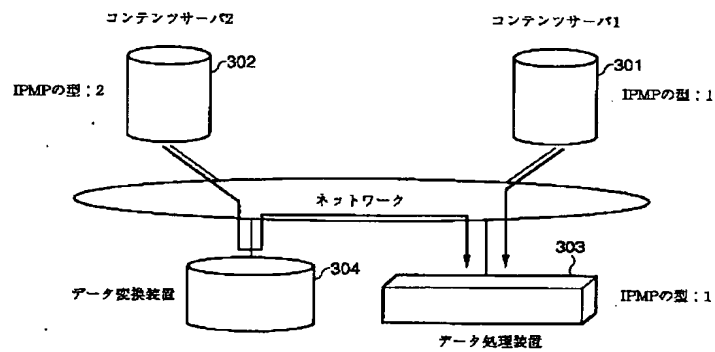
【図1】



【図2】



【図3】

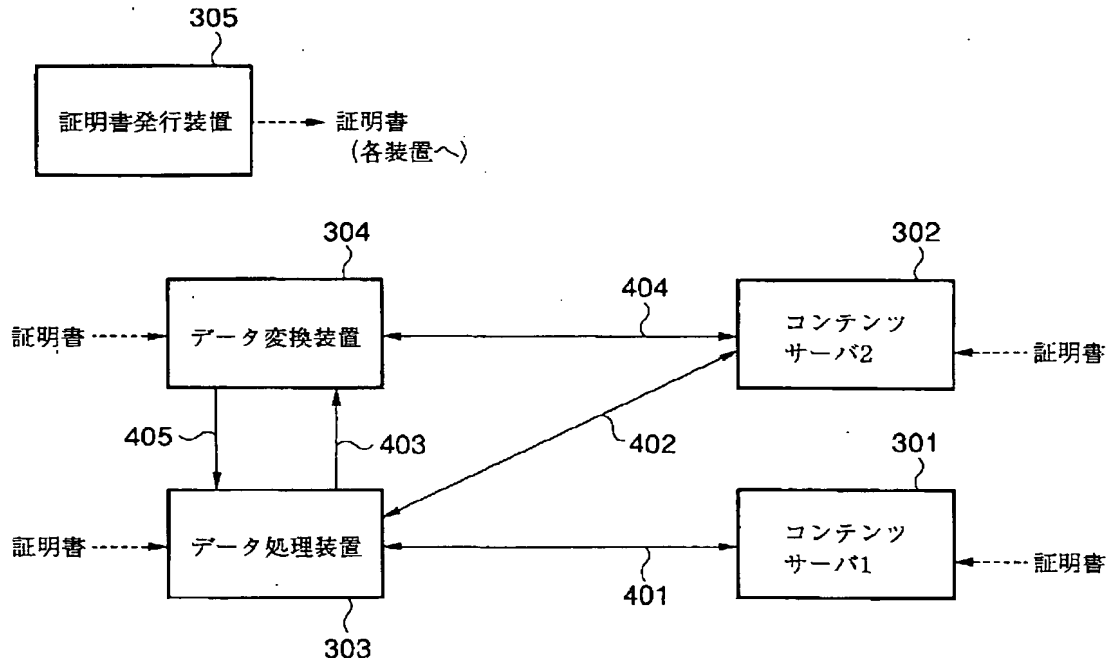


【図6】

ユーザ名	ユーザID	送信コンテンツID	送信日時	隣データの送信
ABC	00001	100000	2000/01/01	0x1234567
DEF	00002	200000	2000/01/02	無し
*****	*****	*****	*****	

← 1ブロック

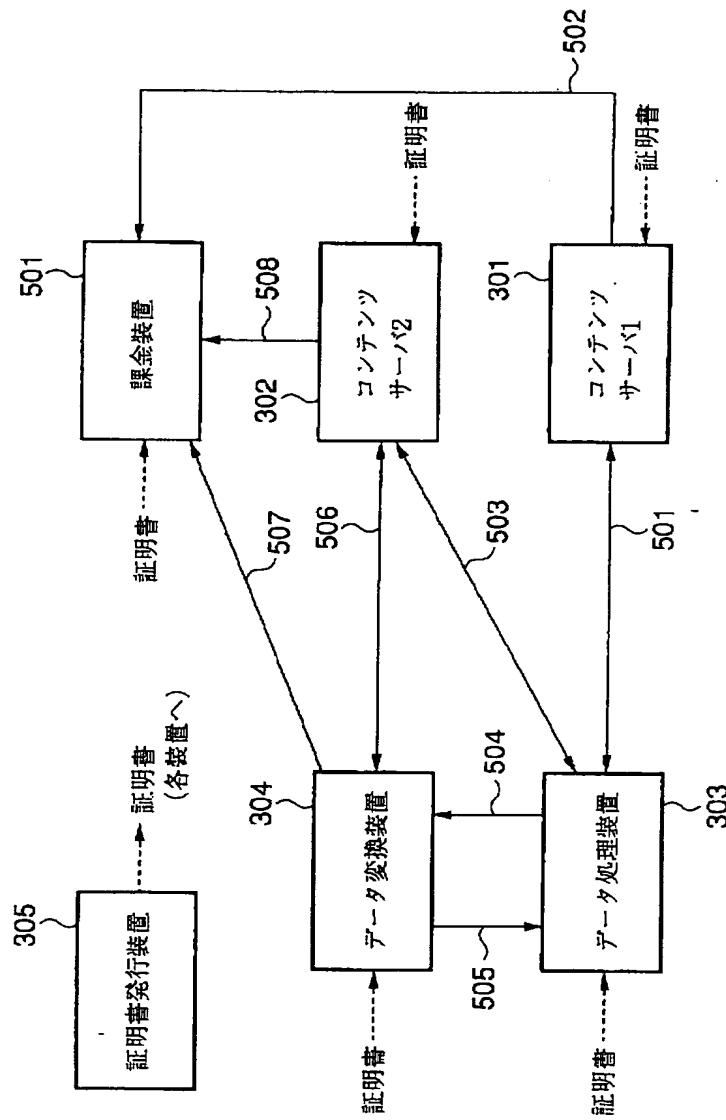
【図4】



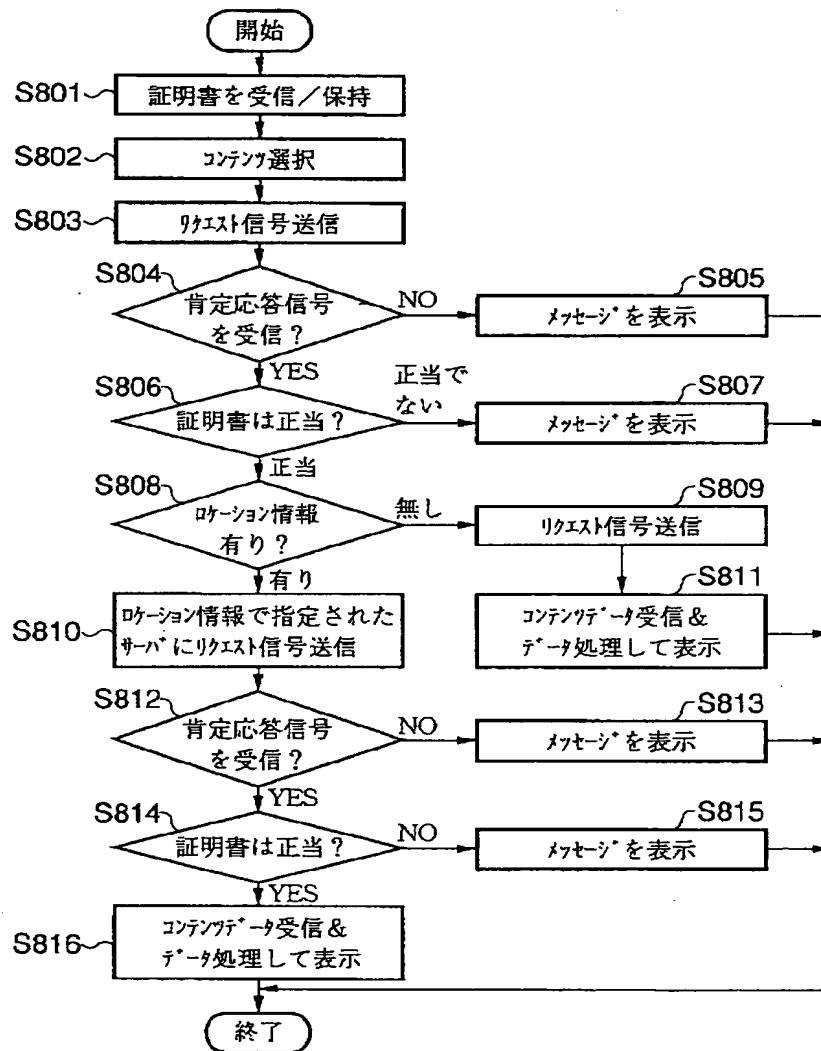
【図7】

ユーザ名	ユーザID	送信コンテンツID	送信日時	変換データ量	変換したIPMPタイプ	変換データの送信
ABC	00001	100000	2000/01/01	10MByte	2→1	0x7654321
DEF	00002	200000	2000/01/02	20MByte	1→2	無し
.....

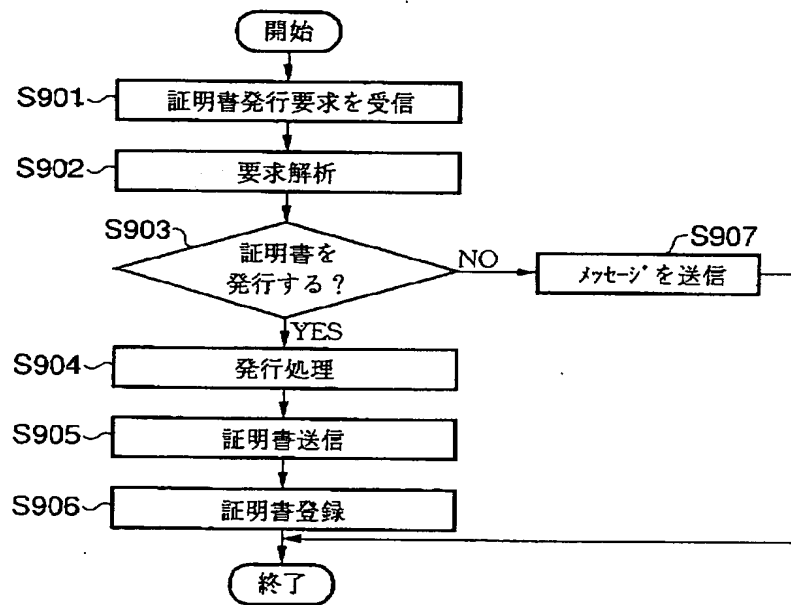
【図5】



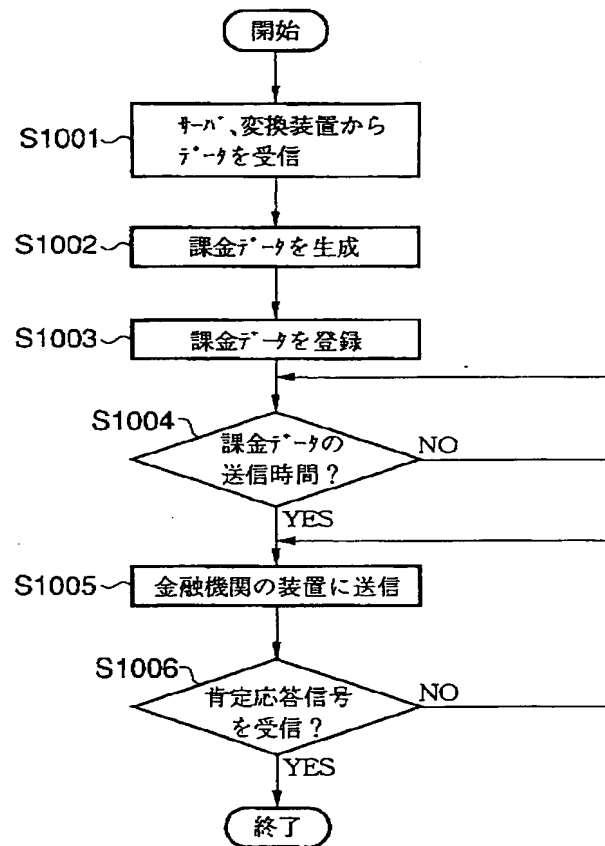
【図8】



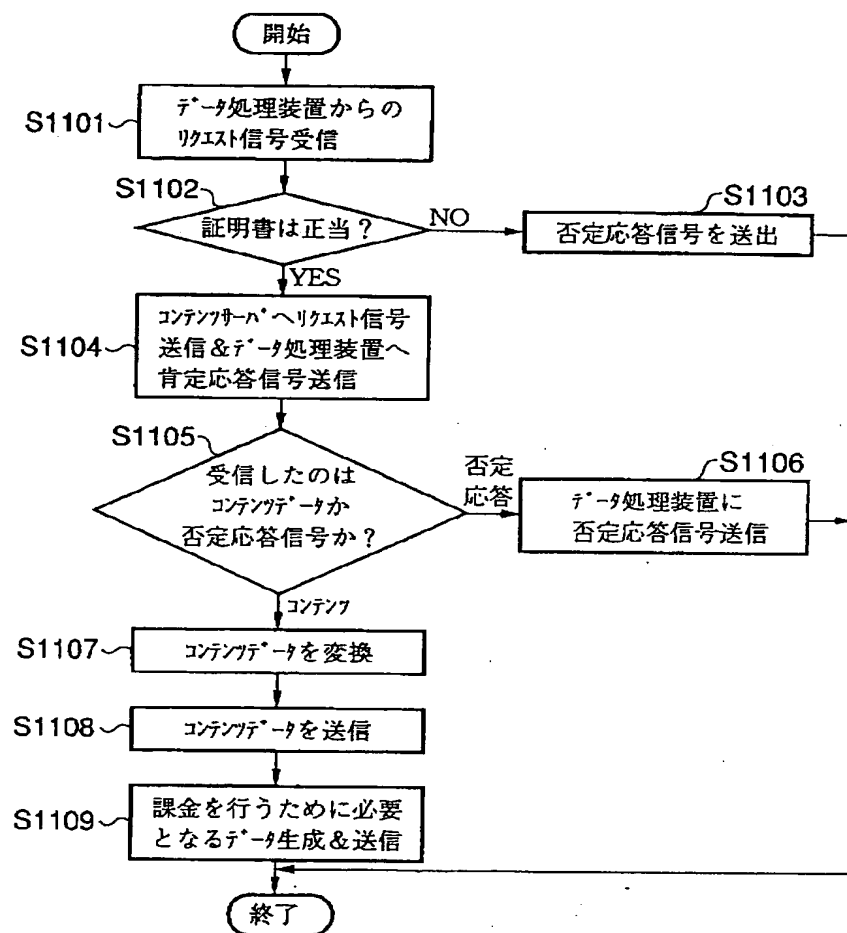
【図9】



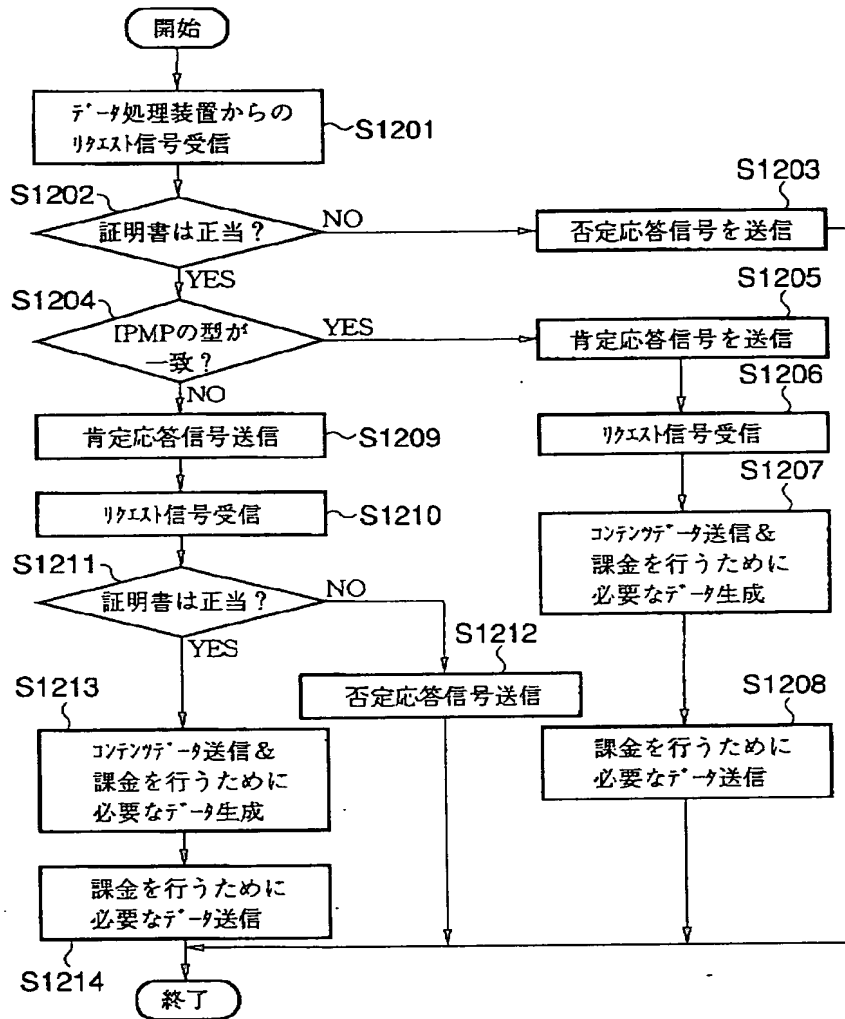
【図 10】



【図11】



【図 12】



フロントページの続き

(51) Int. Cl. 7

G 0 6 F 17/60

識別記号

1 4 2

3 0 2

3 3 2

F I

G 0 6 F 17/60

ターマコード (参考)

1 4 2

3 0 2 E

3 3 2